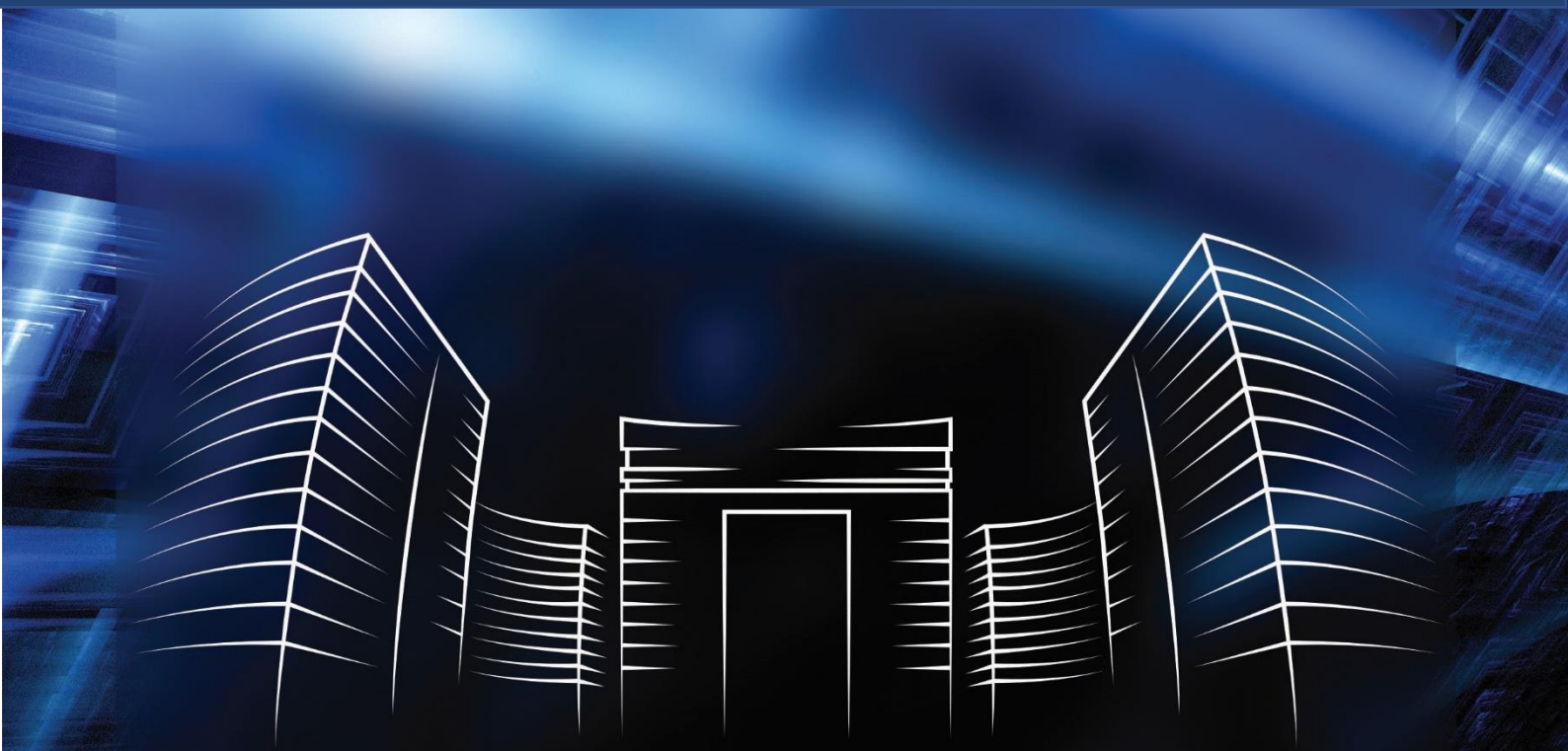
SETIC
Superintendência Estadual de Tecnologia da Informação e Comunicação

Governo do Estado de RONDÔNIA

GUIA DE CONFORMIDADE: LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)



PORTO VELHO/RO - 2021

GUIA DE CONFORMIDADE:
LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

SUPERINTENDÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Delner Freire

Superintendente

DIRETORIA TÉCNICA DA SETIC

Maico Moreira da Silva

Diretor Técnico

ELABORAÇÃO DO GUIA DE CONFORMIDADE

Tiago Lopes de Aguiar

Encarregado pelo Tratamento de Dados Pessoais

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autoria
07/06/2021	1.0	Primeira versão do Guia de Conformidade: Lei Geral de Proteção de Dados Pessoais (LGPD).	Tiago Lopes de Aguiar

SUMÁRIO

INTRODUÇÃO

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade, bem como o livre desenvolvimento da personalidade da pessoa natural. Dispõe sobre o tratamento de dados pessoais realizado por pessoa natural ou por pessoa jurídica (pública ou privada), abrangendo inclusive o tratamento realizado nos meios digitais. Está em vigor em quase sua totalidade, faltando apenas as sanções administrativas, com previsão para 01/08/2021.

Como bem esclarecido no art. 23, LGPD, a administração pública, no tratamento de dados pessoais, deverá atender “sua finalidade pública, na persecução do interesse público, com objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público”. Deve ainda informar as hipóteses em que realiza o tratamento de tais dados, fornecendo informações sobre a previsão legal, finalidade, procedimentos e práticas utilizadas, bem como indicar um encarregado pelo tratamento desses dados.

Nesse sentido, a LGPD constitui marco importante para os órgãos da administração pública, sejam municipais, estaduais ou federais, pois devem cumprir com seus ditames. Dentre suas características, destaca-se a transdisciplinaridade, pois permeia os mais variados órgãos e departamentos na administração pública, cujo tratamento de dados pessoais pode envolver diferentes titulares, desde os próprios servidores até usuários dos serviços públicos.

Portanto, a Superintendência Estadual de Tecnologia da Informação e Comunicação (SETIC), como parte integrante da administração pública do Estado de Rondônia, objetivando entrar em conformidade perante as exigências da LGPD, agindo com responsabilidade e transparência, apresenta o “Guia de Conformidade: Lei Geral de Proteção de Dados (LGPD)”.

Este Guia, construído com base em normas de boas práticas, experiências de especialistas na área e guias operacionais do Governo Federal, tem por objetivo descrever o conjunto das principais ações voltadas para alcançar a conformidade com a LGPD, buscando facilitar a difusão do conhecimento para todos os servidores e departamentos da SETIC. Destaca-se

que foi desenvolvido considerando as peculiaridades da SETIC, tais como área de atuação, organização, estrutura, atribuições etc. Entretanto, seu conteúdo poderá ser utilizado por outro órgão, que deverá atentar para as possíveis adaptações perante sua realidade.

O conjunto de ações se resume em 7 (sete) etapas, a saber:

1. Conhecer as peculiaridades do negócio;
2. Realizar workshop com alta administração, diretoria e coordenadorias das áreas de negócio;
3. Conduzir mobilização inicial;
4. Inventariar dados pessoais;
5. Desenvolver parecer diagnóstico;
6. Criar plano de ação;
7. Executar plano de ação (implementação).

A **Figura 1** apresenta, de forma sintetizada, cada uma dessas etapas, que serão detalhadas mais adiante.

Figura 1 - Etapas para conformidade com LGPD

1. PECULIARIDADES DO NEGÓCIO

A primeira etapa em busca da conformidade com a LGPD consiste em conhecer as peculiaridades do órgão, elencando suas finalidades e competências, bem como evidenciando sua área de atuação e funcionamento.

Fonte: Pixabay

Nesse sentido, é importante o levantamento dos seguintes itens:

- normativas que tratam da organização e estrutura do órgão, abrangendo sua criação, atribuições, competências, regimento interno etc.;
- normativas aprovadas, ou que estão em fase de aprovação, que tratem de política de privacidade, termos de uso, política de segurança da informação, procedimentos de backup, modelos de contrato de trabalho e prestação de serviço, modelos de termos de compromisso, uso de repositórios, uso de mídias sociais, acesso remoto, desenvolvimento seguro de softwares, procedimentos de compras etc.;
- relações com clientes, parceiros, fornecedores, prestadores de serviço, acordos de cooperação, contratos etc.;
- ações existentes, ou já realizadas, visando a adequação do órgão à LGPD tais como workshops, treinamentos, reuniões, nomeação de encarregado pelo tratamento de dados pessoais etc.

Esse levantamento permitirá consolidar as informações iniciais sobre o órgão evidenciando sua organização, estrutura e atribuições. De posse dessas informações, a equipe responsável pela adequação, terá uma melhor compreensão sobre o atual cenário do órgão.

Esta etapa poderá ser conduzida por qualquer pessoa, recomendando-se, entretanto, que seja o futuro encarregado pelo tratamento de dados pessoais ou por pessoas que comporão equipe correlata.

1.1. Diagnóstico inicial

O diagnóstico inicial tem por objetivo mensurar o grau de maturidade do órgão no que diz respeito à conformidade com a LGPD. Os dados coletados nesta 1ª etapa (peculiaridades do negócio) serão muito úteis para o desenvolvimento do diagnóstico inicial, pois será possível perceber as ações que o órgão já executa, que iniciou o planejamento ou ainda que deverão ser idealizadas.

Dentre as diversas ferramentas existentes para realizar o diagnóstico de maturidade, recomenda-se o uso do **Diagnóstico de Adequação à LGPD**[1], disponível pelo Governo Federal, por intermédio da Secretaria de Governo Digital (SGD). Tratando-se de um questionário que, após respondido, apresenta um índice de maturidade, possibilitando a priorização das ações necessárias para entrada em conformidade com a LGPD. O diagnóstico traz consigo o índice de maturidade e seu nível de adequação correspondente, conforme **Figura 2** abaixo:

Índice	Nível de Adequação
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em aprimoramento
0,90 a 1,00	Aprimorado

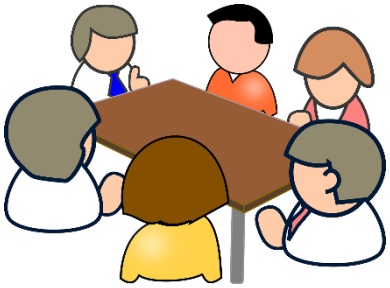
Figura 2 - Índice de adequação à LGPD (Governo Federal, SGD)

Importante destacar é que esse diagnóstico deverá ser repetido em outras etapas, comparando os resultados, com intuito de avaliar o progresso do órgão em busca da conformidade. É um instrumento que permite inclusive demonstrar para a autoridade máxima do órgão, bem como para seus demais líderes, os resultados das ações.

Destaca-se que tal ferramenta é apenas sugestiva, pois, dependendo das peculiaridades do órgão pode ser que outras sejam mais adequadas.

[1] *Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/diagnostico-de-adequacao-a-lgpd. Acesso em: 16 mar. 2021.*

2. WORKSHOP



Fonte: Pixabay

A etapa seguinte, é a realização de *workshop* com a autoridade máxima do órgão, participando também a diretoria e os demais líderes departamentais.

O objetivo é explanar para toda a liderança do órgão, bem como sensibilizá-los, sobre a importância da entrada em conformidade com a LGPD, abordando brevemente sobre seus principais tópicos (entrada em vigor, tratamento de dados pessoais pelo poder público, agentes de tratamento, encarregado pelo tratamento de dados pessoais e boas práticas). Salienta-se que os demais tópicos da LGPD poderão ser objeto de estudos por meio de outros *workshops* ou treinamentos temáticos, inclusive abrangendo todos os demais servidores do órgão.

Os líderes deverão estar cientes de que será necessário a realização de entrevistas no decorrer do processo de conformidade, objetivando a compreensão do fluxo de dados pessoais nos departamentos do órgão.

Destaca-se que a alta administração necessita dar o suporte necessário para que as ações visando a conformidade com a LGPD sejam planejadas e executadas. Esse suporte também refletirá no comportamento dos liderados, que terão seus líderes como exemplo. Nessa etapa já se inicia o processo de mudança cultural no que tange o tratamento de dados pessoais, por meio da conscientização quanto a importância que a LGPD traz para a administração pública, bem como de sua transdisciplinaridade.

Também é oportuno que seja apresentado o *roadmap*, ou seja, as ações necessárias para entrada em conformidade. Neste Guia, o *roadmap* se traduz nas 7 (sete) etapas presentes na **Figura 1**.

Os líderes deverão ser orientados de que a conformidade com a LGPD não se resume em uma única ação, tal como a aquisição de um sistema ou a incorporação ou alteração de um procedimento, mas sim de um conjunto de ações que envolvam estratégia, governança, políticas, procedimentos, ferramentas, gestão de mudança, conscientização, treinamento, monitoramento, responsabilidade, transparência etc.

Esta etapa poderá ser conduzida por qualquer pessoa, recomendando-se, entretanto, que seja o futuro encarregado pelo tratamento de dados pessoais ou por pessoas que comporão equipe correlata.

3. MOBILIZAÇÃO INICIAL

A mobilização inicial se resume na nomeação do encarregado pelo tratamento de dados pessoais, na criação de comissão tática e operacional e na criação de comitê, que farão frente aos trabalhos de conformidade para com a LGPD. Esses atores deverão ser instituídos para atuar no âmbito do órgão que pretende entrar em conformidade.

Fonte: Pixabay

Importante destacar que existem diferentes maneiras de fazer frente aos trabalhos de conformidade, incluindo a criação do grupo e do comitê citados. Entretanto, considerando as peculiaridades da SETIC, decidiu-se criar a Comissão Tática e Operacional e o Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD).

Nessa etapa também será preciso trabalhar a ampla divulgação para o órgão, ou seja, a divulgação interna, explicitando o início da jornada de conformidade e apresentando os profissionais e equipes que estarão conduzindo o processo, bem como realizar outros diagnósticos de adequação à LGPD, com o objetivo de identificar o progresso.

3.1. Encarregado pelo Tratamento de Dados Pessoais

O encarregado pelo tratamento de dados pessoais, conforme apresenta o inciso VIII, art. 5º, LGPD, é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre controlador, titulares e Autoridade Nacional de Proteção de Dados (ANPD), conforme se verifica na **Figura 3**:

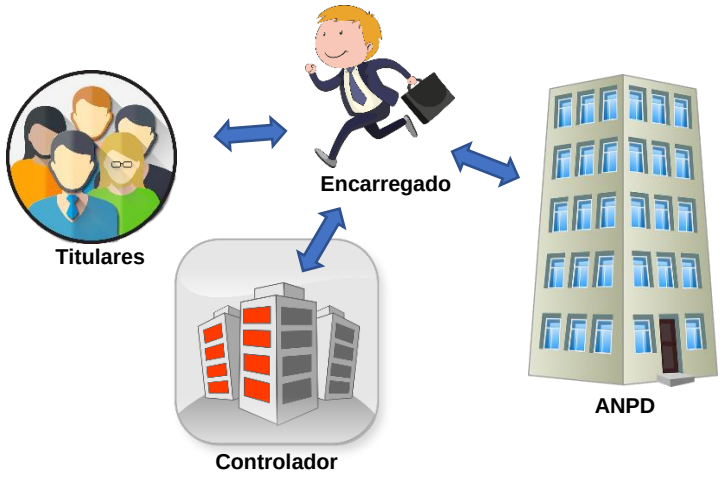


Figura 3: Encarregado pelo Tratamento dos Dados Pessoais

Muitas vezes o encarregado também é chamado de *Data Protection Officer* (DPO), uma tradução para Oficial de Proteção de Dados, nomenclatura utilizada na legislação europeia que também versa sobre privacidade e proteção de dados pessoais, que inclusive foi referência para a criação da LGPD. Entretanto, é importante reforçar que algumas de suas atribuições são diferentes.

A nomeação do encarregado é requisito para que o poder público possa realizar o tratamento de dados pessoais, conforme explicitado no art. 23, III, e *caput* do art. 41, ambos da LGPD, devendo ser indicado pela figura do controlador.

Vale ressaltar que também é mandatória a divulgação pública da identidade e informações de contato do encarregado, atendendo os requisitos da clareza e objetividade, preferencialmente no sítio eletrônico do controlador, conforme ditames do § 1º, art. 41, LGPD.

Conforme **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**[2], o "encarregado é o indivíduo responsável por garantir a conformidade de uma organização, pública ou privada, à LGPD. Tal Guia também explica que o encarregado pode ser "tanto um funcionário da instituição quanto um agente externo, de natureza física ou jurídica", recomendando sua indicação por meio de ato formal (contrato ou ato

[2] *Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 6 jun. 2021, p. 22.*

administrativo). O Guia sugere que o tenha recursos adequados para realização de suas atividades: recursos humanos (equipe de proteção de dados), prazos razoáveis, recursos financeiros e de infraestrutura.

Suas atribuições estão previstas no § 2º, art. 41, LGPD:

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

O encarregado deve ter autonomia e independência para executar suas atribuições, sugerindo-se, inclusive, que tenha acesso direto à autoridade máxima do órgão. No **Guia de Elaboração de Programa de Governança em Privacidade**[3], da Secretaria de Governo Digital (SGD), verifica-se alguns atributos importantes quanto ao encarregado:

- Independência para determinar a aplicação de recursos e as ações necessárias;
- Amplo acesso a estrutura organizacional;
- Pronto apoio das unidades administrativas;
- Investigar os níveis de conformidade (diagnóstico);
- Instruir os responsáveis pelos riscos a corrigir as lacunas encontradas;
- Apoio da alta administração;
- Autonomia e independência funcional.

A escolha do encarregado pelo tratamento de dados pessoais deve levar em conta seus conhecimentos multidisciplinares nas áreas de: gestão,

[3] *Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf. Acesso em: 16 mar. 2021, p. 10-14.*

legislação, tecnologia da informação, segurança da informação, governança de dados etc.

3.2. Agentes de Tratamento

Apesar de não ser o intuito deste Guia de Conformidade, torna-se importante tratar dos conceitos básicos dos agentes de tratamento, uma vez que são referenciados no decorrer dos trabalhos de conformidade.

Os agentes de tratamento são o controlador e o operador, conforme definição trazida no art. 5º, IX, LGPD.

O **controlador** é “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (art. 5º, VI, LGPD), já o **operador** é “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (art. 5º, VII, LGPD).

O **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**[4] esclarece que o controlador, como pessoa jurídica de direito público, Administração Pública Direta, possui obrigações que são distribuídas entre as principais unidades administrativas despersonalizadas que a integram e realizam o tratamento de dados pessoais. Nesse sentido, por força da desconcentração administrativa, nas operações de tratamento conduzidas por órgãos públicos despersonalizados, a pessoa jurídica de direito público a que os órgãos sejam vinculados é a controladora dos dados pessoais, sendo que o órgão despersonalizado desempenhará funções típicas de controlador.

A título de exemplo, no contexto do Governo do Estado de Rondônia, Poder Executivo, a SETIC desempenha funções típicas de controlador, entretanto o Governo do Estado de Rondônia é o controlador dos dados pessoais, pois a SETIC está vinculada ao Governo.

[4] *Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 6 jun. 2021, p. 7-10.*

O **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**[5] também explica que não são considerados controladores ou operadores os indivíduos subordinados, tais como funcionários, servidores públicos ou equipes de trabalho de uma organização, pois já atuam sob o seu poder diretivo (ANPD, 2021, p. 5).

3.3. Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD)

A constituição de um comitê para deliberações sobre privacidade e proteção de dados pessoais é considerado um importante marco para alcançar a conformidade, considerando-se a transdisciplinaridade da LGPD. Dessa forma, a composição do comitê deve ser multidisciplinar, ou seja, seus membros devem representar as diferentes áreas de negócio do órgão, possuindo conhecimentos distintos.

Pelo fato de o comitê ser multidisciplinar, no que diz respeito a sua composição, se torna importante o desenvolvimento de treinamentos objetivando o nivelamento quanto ao conhecimento, atribuições e funcionamento.

A recomendação é que os membros do comitê não só representem as áreas de negócio do órgão, mas que sejam seus líderes, pois detêm conhecimentos em nível estratégico, tático e operacional do funcionamento de seu departamento. Tais membros também desempenharão papel importante na mudança cultural da organização, pois serão considerados verdadeiros influenciadores quanto ao adequado tratamento de dados pessoais, servindo de referências para seus liderados. Além disso, tais líderes terão poder de voto em deliberações que se referem ao tratamento de dados pessoais, fazendo parte das decisões e diretrizes que o órgão deverá seguir em busca da conformidade com a LGPD.

Recomenda-se ainda que o encarregado pelo tratamento de dados pessoais faça parte da composição do comitê.

---

[5] *Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 6 jun. 2021, p. 5.*

Caso já exista um comitê dentro do órgão, pode-se considerar a possiblidade desse comitê assumir as atribuições relativas às deliberações relacionadas à LGPD, alterando sua norma de criação.

O Comitê Gestor de Privacidade e Proteção de Dados Pessoais (CGPD) tem atuação estratégica e tática frente à conformidade com a LGPD. Dentre suas atribuições destacam-se:

- Colaborar com o desenvolvimento, implementação e execução do Programa de Governança em Privacidade (PGP)
- Assessorar atividades relacionadas ao tratamento de dados pessoais;
- Facilitar a promoção cultural de privacidade e proteção de dados pessoais;
- Avaliar processos e procedimentos que envolvam tratamento de dados pessoais;
- Propor ações e diretrizes voltadas ao tratamento e proteção de dados pessoais;
- Deliberar sobre propostas de medidas destinadas à privacidade e proteção de dados pessoais;
- Auxiliar o encarregado pelo tratamento de dados pessoais no cumprimento de suas competências.

3.4. Comissão Tática e Operacional

A Comissão Tática e Operacional, diferentemente do CGPD, desenvolverá ações operacionais. Seu objetivo principal é a construção de plano de ação para adequação do órgão às exigências da LGPD, bem como a elaboração do Programa de Governança em Privacidade (PGP).

Observem que o plano de ação é a 6ª etapa do *roadmap* apresentado, entretanto, para alcançar essa etapa, a Comissão deverá necessariamente executar as etapas 4 (inventário de dados pessoais) e 5 (parecer diagnóstico), apresentando, ao final, o plano de ação e o PGP.

Periodicamente, a Comissão Tática e Operacional deverá prestar informações sobre o desenvolvimento de seus trabalhos ao CGPD. Ao final dos trabalhos, deverá apresentar os registros de suas atividades, bem como o plano de ação e o PGP ao CGPD, que deliberará sobre suas aprovações.

Deverá ser composto por equipe técnica, sob presidência do Encarregado pelo Tratamento de Dados Pessoais. Sugere-se que, dentre seus membros, hajam pessoas que detenham os seguintes conhecimentos: privacidade e proteção de dados pessoais, mapeamento de processos, análise de risco, gestão de projetos, segurança da informação e direito. Importante também contar com pessoas que darão suporte operacional.

Destaca-se ainda a necessidade de nivelamento quanto às exigências que a LGPD traz para a administração pública, pois é importante que o grupo esteja alinhado.

3.5. Ampla divulgação

A ampla divulgação trata-se da divulgação interna, apresentando para todos os servidores e departamentos do órgão o início da jornada para entrar em conformidade com a LGPD. Deve-se introduzir uma mensagem positiva, enfatizando-se a responsabilidade e o comprometimento do órgão como integrante da administração pública, e que a condução dessa jornada será realizada por profissionais comprometidos, destacando-se o papel do encarregado pelo tratamento de dados pessoais, da Comissão Tática e Operacional e do CGPD.

Essa atitude também tem por objetivo a promoção da mudança cultural no ambiente organizacional, enfatizando-se a responsabilidade quanto ao tratamento de dados pessoais, procurando conscientizar todos os envolvidos.

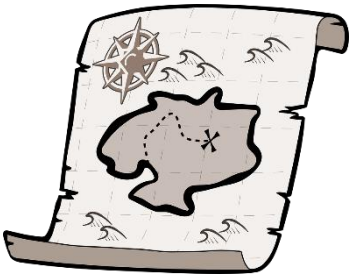
3.6. Diagnósticos intermediários

Os diagnósticos intermediários consistem no uso da mesma ferramenta utilizada no diagnóstico inicial, com intuito de comparar os índices de maturidades e direcionar esforços para consecução de ações específicas para entrada em conformidade com a LGPD.

Recomenda-se realizar quantos diagnósticos forem necessários no decorrer do *roadmap*, incluindo-se nesta última ação da 3ª etapa.

Aqui, já serão consideradas muitas etapas vencidas, tais como o *workshop* com a alta administração, criação de comitê, criação da comissão tática e operacional, nomeação do encarregado pelo tratamento de dados e divulgação interna enfatizando a jornada de conformidade e apresentando os profissionais responsáveis para todo o órgão.

4. INVENTÁRIO DE DADOS PESSOAIS



Fonte: Pixabay

A etapa de Inventário de Dados Pessoais (IDP) é uma das mais importantes na jornada de conformidade. Inclusive esta etapa contempla uma das exigências da LGPD, mais especificamente em seu art. 37, quando determina que "o controlador e o operador devem manter registro de operações de tratamento de dados pessoais que realizarem". Além disso, visa subsidiar a elaboração do Relatório de Impacto de Proteção de Dados Pessoais (RIPD) e outras ações necessárias, como a identificação de lacunas frente às exigências da LGPD ou de outras normas.

O objetivo é realizar o levantamento das ações que o órgão realiza com os dados pessoais, indicando, por exemplo, quais são os dados tratados, onde estão armazenados e quais operações são realizadas.

A metodologia sugerida para realizar o IDP é a *top-down*, iniciando-se a análise pelos serviços/processos, e não pelo dado propriamente dito. Para realizar tal ação, recomenda-se a utilização do **Guia de Elaboração de Inventário de Dados Pessoais**[6], também disponibilizado pela Secretaria de Governo Digital (SGD). Tal guia, conforme suas orientações, foi desenvolvido com base em metodologias adotadas na Bélgica, Inglaterra e França, apresentando um *template* no formato de planilha eletrônica como ferramenta de apoio. Salienta-se que tal guia é apenas sugestivo, e que a planilha deve ser adaptada considerando a realidade de cada órgão.

Os resultados desta etapa irão refletir na avaliação quanto às medidas de segurança e suas aplicações, bem como na mitigação ou resolução de possíveis lacunas.

Dependendo das peculiaridades do órgão, bem como da disponibilidade de recursos humanos e tecnológicos, o IDP poderá ser realizado de diferentes formas. Sugere-se que a Comissão Tática e Operacional, responsável por realizar o IDP, opte pelas seguintes ações, na ordem em que são apresentadas:

[6] *Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaInventario.pdf. Acesso em: 17 mar. 2021, p. 6.*

a) realizar nivelamento de conhecimento com seus próprios membros, por meio de *workshops* e oficinas, a respeito da metodologia adotada para realizar o IDP;
b) solicitar para o CGPD e alta administração que os departamentos do órgão disponibilizem ao menos um representante para conduzir o IDP dentro de seu escopo de atuação;
c) receber a relação de indicados pelos departamentos;
d) realizar o nivelamento de conhecimento com os indicados, por meio de *workshops* e oficinas, sobre o IDP e utilização da ferramenta para sua realização;
e) acompanhar a execução do IDP pelos indicados, inclusive ofertando suporte necessário e sanando dúvidas;
f) receber os registros de operações e revisá-los em conjunto com os indicados, reunindo-se, conforme necessidade, com a liderança do respectivo departamento;
g) sugerir periodicidade de revisão e atualização dos registros de operações de tratamento de dados pessoais.

O IDP deverá ser realizado pelos responsáveis do serviço/processo de negócio, ou seja, por seus donos, com o apoio da Comissão Tática e Operacional. Nesse sentido, a SETIC demandou que cada departamento realizasse o seu IDP, dividindo esforços e poupando tempo, pois se a Comissão Tática e Operacional fosse realizá-lo, teria que perpassar em cada departamento e promover uma série de entrevistas com seus servidores e líderes. Tais ações podem se tornar mais complexas dependendo do tamanho da organização, destacando-se que o ideal seria estabelecer ações de mapeamento e análise de processos antes dessa etapa.

Ao final, a Comissão Tática e Operacional terá os registros das operações de tratamento de dados pessoais considerando cada serviço/processo existem na organização. Destaca-se que é importante sempre manter tais registros atualizados, por isso deve-se estabelecer um ciclo de periodicidade para revisão, bem como a realização de atualização sempre que houver mudança no ciclo de tratamento de dados pessoais do serviço/processo relacionado.

5. PARECER DIAGNÓSTICO

Fonte: Pixabay

Esta etapa se caracteriza pela avaliação e validação do Inventário de Dados Pessoais (IDP), devendo ser apreciadas questões que envolvam, dentre outras: o ciclo de tratamento dos dados pessoais; o fluxo de tratamento; as hipóteses legais; finalidade; previsão legal; os tipos de dados pessoais tratados; frequência de tratamento; as categorias dos titulares; possíveis compartilhamentos; medidas de segurança e privacidade; transferências internacionais; e contratos ou acordos existentes.

Por meio dessa ação a equipe deverá identificar os serviços/processos de negócios que precisam se adequar à LGPD, bem como as lacunas (*gaps*) existentes, recomendando soluções para resolvê-los ou mitiga-los.

É o momento para realizar a avaliação crítica sobre todas as operações de tratamento de dados pessoais que são realizadas pelo órgão. Tais informações subsidiarão a elaboração da próxima etapa, ou seja, do plano de ação para adequação à LGPD.

6. PLANO DE AÇÃO

Com base no parecer diagnóstico, a Comissão Tática e Operacional desenvolverá o Plano de Ação, elencando as atividades necessárias para que o órgão entre em conformidade com as exigências da LGPD, devendo seguir uma ordem de prioridade.

Fonte: Pixabay

Esse parecer deverá ser apresentado ao CGPD, que deliberará por sua aprovação e priorizará as ações que julgar serem mais importantes.

Dentre as ações que poderão ser apresentadas, destacam-se:

	Ação	Justificativa
1	Implementação do Programa de Governança em Privacidade (PGP)	O Programa de Governança em Privacidade (PGP) propõe ações permanentes de conformidade com a LGPD, e está previsto no art. 50, da LGPD. Dentre suas peculiaridades, deve-se atentar ao estabelecimento de políticas e salvaguardas, aplicabilidade a todo o conjunto de dados pessoais, contar com planos de respostas a incidentes e remediações e estabelecer relação de confiança com o titular. Além disso, também deverá propor ações de melhoria contínua no que diz respeito ao cumprimento das diretrizes estabelecidas pela LGPD, sugerindo-se a adoção de um ciclo que estabeleça o monitoramento e auditoria dessas ações.
2	Implementar campanha de publicidade e conscientização	A instituição de uma campanha de publicidade e conscientização é uma ação que visa principalmente a mudança cultural quanto ao tratamento de dados pessoais, uma vez que a LGPD é transdisciplinar e deve ser cumprida no decorrer de todo o ciclo de vida do tratamento de dados pessoais. No mais, na própria LGPD (art. 50, I, “a”) se verifica que o Programa de Governança em Privacidade (PGP) deve demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais, o que poderá ser incentivado por meio da campanha de publicidade e conscientização.

3	Implementar na cultura do órgão o *Privacy By Design*	O *Privacy By Design* consiste em desenvolver projetos, produtos ou serviços já inserindo medidas de privacidade desde a concepção, ou seja, desde sua construção. O *Privacy by Design* possui sete princípios, sendo estes: Proatividade e prevenção; *Privacy by Default* (privacidade como padrão); Privacidade incorporada ao *design*, pois deve ser incorporado ao desenvolvimento e à arquitetura de sistemas de TI, bem como em práticas de negócios e quaisquer produtos e serviços desenhados; Funcionalidade total, pois busca acomodar todos os legítimos interesses e objetivos; Segurança de ponta a ponta, uma vez que integra todas as fases do ciclo de vida do tratamento de dados pessoais; Visibilidade e transparência, que preza pela diligência e pelo *compliance*; e Respeito pela privacidade do usuário. O art. 6º da LGPD elenca um rol de princípios que devem ser observados desde a concepção de um projeto, produto ou serviço, relacionando-se diretamente com o *Privacy by Design*. No mais, a própria LGDP (art. 46, § 2º) determina que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais, sendo que tais medidas devem ser observadas desde a fase de concepção do produto ou do serviço até sua execução.
4	Implementar portfólio de treinamento e desenvolvimento	O treinamento e desenvolvimento consistem em ações objetivando o nivelamento e constante aperfeiçoamento envolvendo boas práticas na conformidade com a LGPD. Consiste numa necessidade, uma vez que a LGPD é transdisciplinar, devendo ser aplicada durante todo o ciclo de vida do tratamento de dados pessoais. No mais, na própria LGPD (art. 50, I, “a”) se verifica que o Programa de Governança em Privacidade (PGP) deve demonstrar o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais, o que poderá ser incentivado por meio de programas de treinamento e desenvolvimento.
5	Desenvolver Relatórios de Impacto de Proteção de Dados (RIPD)	De acordo com o art. 5º, XVII, LGPD, o Relatório de Impacto de Proteção de Dados (RIPD) consiste em “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco”. Ademais, ao longo da LGPD, o RIPD é abordado em diferentes vertentes. No art. 4º, § 3º, a ANPD deverá solicitá-lo aos responsáveis elencados no rol de exceções do art. 4º, III. No art. 10, § 3º, a ANPD poderá solicitá-lo quando do tratamento com fundamento no legítimo interesse. No art. 32, a ANPD poderá solicitar sua publicação e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público. No art. 38, a ANPD poderá determinar ao controlador sua elaboração referente a operações de tratamento de dados pessoais.

6	Criar procedimentos para manter o IDP atualizado	Conforme Guia de Elaboração de Inventário de Dados Pessoais (SGD, 2021, p. 25), o Inventário de Dados Pessoais (IDP) é um documento “vivo”, que deve ser atualizado, no mínimo, anualmente, ou sempre que existir mudanças no tratamento de dados pessoais do serviço/processo inventariado. Destaca-se que é importante sempre manter tais registros atualizados, por isso deve-se estabelecer um ciclo de periodicidade para revisão, bem como a realização de atualização sempre que houver mudança no ciclo de tratamento de dados pessoais do serviço/processo relacionado. No mais, o art. 37 da LGPD versa que “O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem [...]”
7	Elaborar modelo de política de privacidade	A Política de Privacidade, conforme Guia de Elaboração de Termo de Uso e Política de Privacidade para Serviços Públicos (SGD, 2020, p. 24), tem como objetivo descrever ao usuário o método, os processos e os procedimentos adotados no tratamento de dados pessoais pelo serviço e informá-lo sobre as medidas de privacidade empregadas. Para isso, o serviço deve informar ao titular do dado como ele fornece a privacidade necessária para que a confidencialidade dos dados prestados pelos titulares seja garantida de forma eficiente e como os princípios elencados no art. 6º, LGPD, são atendidos. O art. 6º, que trata dos princípios da LGPD, traz em seu inciso VI o princípio da transparência, o qual consiste em “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”, justificando a implementação da Política de Privacidade. Ademais, o *caput* do art. 50 da LGPD versa que os controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam, dentre outros, regime de funcionamento, normas de segurança e outros aspectos relacionados ao tratamento de dados pessoais, reforçando a ideia da implementação da Política de Privacidade.

8	Instituir a gestão de incidentes de violação de dados pessoais	Considerando as diretrizes que a LGPD nos traz, é importante frisar que o controlador deverá comunicar à ANPD, bem como ao titular, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, inteligência do *caput*, art. 48, LGPD. Já o art. 48, § 1º, estabelece que tal comunicação deverá ser realizada em prazo razoável, contendo no mínimo: a descrição da natureza dos dados pessoais afetados; informações sobre os titulares envolvidos; e indicação das medidas técnicas e de segurança utilizadas para proteção dos dados. Dessa forma, torna-se imperiosa a implementação de uma gestão de incidentes de violação de dados pessoais, abrangendo a criação de: um CSIRT (Computer Security *Incident Response Team* - Grupo de Resposta a Incidentes de Segurança); de procedimentos para apuração de incidentes; de gestão de auditoria e *logs*; e plano de respostas e comunicação de incidentes. Com tais ações, o órgão também estará cumprindo com as determinações contidas no art. 50, § 2º, I, "g", LGPD, que consiste na abordagem de planos de respostas a incidentes e remediações no Programa de Governança em Privacidade (PGP). O órgão também deverá promover o registro das ações adotadas para solucionar os incidentes que envolvam violação de dados pessoais, bem como registrar tais incidentes, tornando-se importante o estabelecimento de responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes que envolvam violação de dados pessoais.
9	Elaborar modelo de termo de uso	O Termo de Uso, conforme Guia de Elaboração de Termo de Uso e Política de Privacidade para Serviços Públicos (SGD, 2020, p. 6), é um documento que estabelece as regras e condições de uso de determinado serviço. Caso o Termo de Uso seja aceito pelo usuário, a utilização do serviço será vinculada às cláusulas dispostas nele. O art. 6º, que trata dos princípios da LGPD, traz em seu inciso VI o princípio da transparência, o qual consiste em "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial", justificando a implementação do Termo de Uso. Ademais, o *caput* do art. 50 da LGPD versa que os controladores e operadores poderão formular regras de boas práticas e de governança que estabeleçam, dentre outros, regime de funcionamento, normas de segurança e outros aspectos relacionados ao tratamento de dados pessoais, reforçando a ideia da implementação da Termo de Uso.

10	Criar canal para contatar o encarregado e para realizar denúncias, incluindo a possibilidade de comunicação em modo anônimo	A institucionalização de canal para contatar o encarregado, bem como para registro de denúncias, pressupõem ação voltada à auditoria e ao monitoramento no que diz respeito à conformidade do tratamento de dados pessoais perante a LGPD e o cumprimento dos princípios elencados no art. 6º da referida Lei. O art. 5º, VIII, LGPD, contém a definição de encarregado, que consiste: "Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD". Ademais, o art. 50, § 2º, I, alínea "e", esclarece que no Programa de Governança em Privacidade (PGP) tem o "objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular". O caráter da denunciação anônima busca proteger a identidade da pessoa do denunciante, evitando perseguições e retaliações. Portanto, para cumprir tais apontamentos deve-se instituir canal de comunicação para contar o encarregado, bem como para apuração de eventuais desvios.
11	Adquirir ou desenvolver sistema para gerir requisições e consentimento de titulares	De acordo com o art. 18 da LGPD, o titular tem direito a obter do controlador, em relação aos seus dados pessoais, a qualquer momento e mediante requisição: a confirmação da existência de tratamento; o acesso aos dados; a correção de dados; a anonimização, bloqueio ou eliminação de dados; a portabilidade dos dados a outro fornecedor de serviço ou produtos; a eliminação dos dados pessoais tratados com o consentimento do titular; a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e a revogação do consentimento. O titular também tem direito à revisão de decisões automatizadas (art. 20, LGPD). Sobretudo, destaca-se que o titular exercerá seus direitos mediante requerimento expresso dele próprio ou de representante legalmente constituído, a agente de tratamento (art. 18, § 2º, LGPD). Segundo Viviane Maldonado, "A gestão é sim algo complexo, mas a preparação inicia com o agente de tratamento elencando e organizando tudo aquilo que seja necessário para se conseguir responder ao titular. A gestão das requisições passará basicamente por três aspectos, que devem acontecer ao mesmo tempo. Primeiro, por processos, com canal para receber as demandas e desenhados a partir da realidade de cada empresa. Segundo, por treinamentos, para toda a pirâmide da organização. E terceiro, mas não menos importante, é preciso facilitar para o titular". Portanto, torna-se imperioso que a o órgão implemente tal sistema, capaz de gerir as requisições dos titulares, bem como seu consentimento, permitindo gerar registros de auditoria no que diz respeito ao exercício de seus direitos.

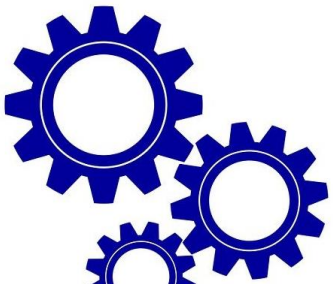
12	Revisar contratos com parceiros e terceirizados	A adequação e revisão dos atuais contratos com terceiros deve ser realizada objetivando o cumprimento dos dispositivos da LGPD, tanto pelo controlador quanto pelo operador, e demais envolvidos no tratamento de dados pessoais. Nesse sentido, deve-se procurar atender principalmente aos princípios da adequação, responsabilização e prestação de contas, elencados no art. 6º, LGDP, buscando cumprir com a compatibilidade entre o tratamento e as finalidades elencadas em contrato, bem como com a observância e o cumprimento de normas de proteção de dados pessoais pelos envolvidos no ciclo de tratamento. A LGPD, em seu artigo 42, *caput*, determina que a responsabilidade por qualquer dano ou violação referente ao tratamento de dados pessoais é do controlador ou operador. Inclusive há previsão (art. 42, I, LGPD) de responsabilidade solidária do operador quando este não cumprir com suas obrigações legais e com instruções lícitas do controlador. Dessa forma, torna-se imperioso que todos os contratos, termos, convênios e congêneres estejam adequados à LGPD e normas complementares e conexas, prevendo cláusulas específicas sobre proteção de dados pessoais, destacando-se ainda a necessidade de realizar diligências junto aos parceiros para validação de cumprimento das exigências da LGPD (*Due Diligence*).
13	Proceder com a criação e utilização de métricas (KPI)	As métricas possibilitam mensurar, monitorar e gerir as estratégias para que possamos entrar em conformidade com a LGPD. Elas apresentam informações sobre quais estratégias devem ser continuadas, aperfeiçoadas ou até mesmo abandonadas. Conforme o Programa de Governança em Privacidade do Ministério das Comunicações (Disponível em: https://www.gov.br/mcom/pt-br/composicao/secretaria-executiva-novo/planejamento-e-tecnologia-da-informacao/programa-de-governanca-em-privacidade. Acesso em: 27 mai. 2021), as métricas são ferramentas que facilitam a tomada de decisões estratégicas e a prestação de contas. São obtidas mediante a coleta, análise e relatório de dados. Para serem eficientes, devem ser objetivas, mensuráveis, relevantes e claramente definidas, além de alinhadas com objetivos específicos do Programa de Governança em Privacidade. O ciclo de vida da métrica envolve a identificação da audiência a que as métricas se destinam, seleção das métricas relevantes, definição dos responsáveis por sua mensuração, coleta e análise da métrica. São essenciais pois apontam os reais resultados de investimentos, sejam em gestão de pessoas, otimização de processos, redução de gastos, aumento da produtividade dentre outros. São exemplos de métricas: percentual de treinamentos concluídos; porcentagem de conformidade de sistemas; número de requisições de titulares de dados; número de incidentes de segurança/vazamento de dados etc. Considerando a avaliação diagnóstica da SGD, abrange 1 dos seus quesitos (B7).

14	Implementar gestão de vulnerabilidades	A gestão de vulnerabilidades objetiva a realização de monitoramento e aplicação de resolução/mitigação de eventuais falhas existentes em sistemas inseridos no contexto do órgão. Procura prevenir a exploração de tais vulnerabilidades, identificando e aplicando soluções específicas. O órgão deve adotar ou reforçar as ações de gestão de vulnerabilidades, procurando cumprir com a abordagem contida no *caput* do art. 50, LGPD, que determina que tanto o controlador quanto o operador deverão formular regras de boas práticas e de governança que estabeleçam mecanismos internos de supervisão e de mitigação de riscos. A análise de vulnerabilidades, por exemplo, deve ser realizada periodicamente, registrando e notificando os envolvidos, e orientando-os quanto ao seu uso, manutenção e desenvolvimento. Nesse contexto, o órgão deve adotar mecanismos de monitoramento proativo no que diz respeito aos eventos de segurança. Não obstante, tal ação também visa o atendimento do previsto no *caput* do art. 46 da LGPD, determinando que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".
15	Implementar a avaliação de riscos de segurança e de privacidade	A avaliação de riscos de segurança e de privacidade deve ocorrer com base nos Relatórios de Impacto de Proteção de Dados (RIPD), que dependem da realização do Inventário de Dados Pessoais (IDP). Risco, conforme "Glossário de Segurança da Informação" (Portaria nº 93, de 26 de setembro de 2019), consiste num "potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização". Já a avaliação de riscos consiste no "processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco". A avaliação de riscos objetiva classificar os riscos envoltos dos ativos, neste caso os dados pessoais dos titulares, e possibilitar a implementação de ações voltadas à mitigação, resolução ou transferência do risco. Não obstante, o órgão deve cumprir com a abordagem contida no *caput* do art. 50, LGPD, que determina que tanto o controlador quanto o operador deverão formular regras de boas práticas e de governança que estabeleçam mecanismos internos de supervisão e de mitigação de riscos.

16	Implementar Política de Segurança da Informação (PSI)	Política de Segurança da Informação (PSI), conforme "Glossário de Segurança da Informação" (Portaria nº 93, de 26 de setembro de 2019), consiste num documento contendo um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação. Conforme descreve o art. 46 da LGPD: "Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". A adoção de uma PSI também cumpre com os quesitos elencados no art. 50, § 1º, I, "a" e "d", especificando que o controlador deve demonstrar comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; e estabelecer políticas e salvaguardas adequadas. Dessa forma, a implementação de uma PSI procura prevenir danos ao andamento do negócio e padronizar procedimentos, além de prever e mensurar respostas a incidentes. A longo prazo, isso pode resultar na redução de custos com incidentes de TIC. A PSI deve estar de acordo com os requisitos de negócio e com leis e regulamentações aplicáveis, devendo conter, além dos objetivos, princípios e requisitos do documento, as seguintes normatizações: responsabilidades dos servidores; responsabilidades da área de TIC; informações ligadas à logística da implementação da TIC no órgão; tecnologias de defesa contra ciberataques; política de treinamento aos colaboradores dentre outras.

O rol acima é apenas exemplificativo, podendo haver outras ações necessárias para que o órgão entre em conformidade com a LGPD.

7. IMPLEMENTAÇÃO



Fonte: Pixabay

De posse do plano de ação, o órgão, por intermédio do CGPD e do Encarregado pelo Tratamento de Dados Pessoais, executará as ações previstas objetivando sua adequação à LGPD, considerando a ordem de priorização.

Dentre as ações, é importante destacar a implementação do Programa de Governança em Privacidade (PGP), no qual o CGPD deliberará sobre sua aprovação, pois proporcionará ações permanentes com vistas à conformidade com a LGPD, visando a melhoria contínua.

REFERÊNCIAS

BRASIL. **Guia de boas práticas**: Lei Geral de Proteção de Dados Pessoais (LGPD). Comitê Central de Governança Digital. Versão 2. Brasília: ago. 2020.

BRASIL. **Guia de elaboração de inventário de dados pessoais**. Ministério da Economia. Secretaria de Governo Digital (SGD). Brasília: abr. 2021. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia_inventario_dados_pessoais.pdf. Acesso em: 6 jun. 2021.

BRASIL. **Guia de elaboração de programa de governança em privacidade**. Ministério da Economia. Secretaria de Governo Digital (SGD). Brasília: out. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf. Aceso em: 6 jun. 2021.

BRASIL. **Guia de elaboração de termo de uso e política de privacidade para serviços públicos**. Ministério da Economia. Secretaria de Governo Digital (SGD). Brasília: set. 2020. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaTermoUso.pdf. Acesso em: 6 jun. 2021.

BRASIL. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. ANPD. Brasília: mai. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/2021-05-27-guia-agentes-de-tratamento_final.pdf. Acesso em: 6 jun. 2021.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Aceso à Informação (LAI). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm. Acesso em 28 mar. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 28 mar. 2021.

BRASIL. **Portaria nº 93, de 26 de setembro de 2019**. Aprova o Glossário de Segurança da Informação. Presidência da República/Gabinete de Segurança Institucional. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663. Acesso em 6 jun. 2021.

BRASIL. **Programa de Governança em Privacidade do MCOM**. Ministério das Comunicações. Disponível em: https://www.gov.br/mcom/pt-br/composicao/secretaria-executiva-novo/planejamento-e-tecnologia-da-informacao/programa-de-governanca-em-privacidade/ProgramadeGovernanaemPrivacidadedoMCaLGPD_mcom.pdf. Acesso em: 6 jun. 2021.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

CRESPO, Marcelo Xavier de Freitas. **Compliance no Direito Digital**. São Paulo: Thomson Reuters Brasil, v. 3, 2020.

MALDONADO, Viviane Nóbrega. LGPD: **Lei Geral de Proteção de Dados Pessoais**: manual de implementação. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

MALDONADO, Viviane. SERPRO Notícias e Artigos. **O titular e a gestão de seus direitos**. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/titular-gestao-direitos-lgpd/. Acesso em: 6 jun. 2021.

OLIVEIRA, Ricardo; COTS, Márcio. **O legítimo interesse e a LGPDP**. 1. ed. São Paulo: Thomson Reuters Brasil, 2020.

PINHEIRO, Patricia Peck. **Direito digital**. 6. ed. São Paulo: Saraiva, 2016.
POZZO, Augusto Neves Dal. MARTINS, Ricardo Marcondes. **LGPD e administração pública**: uma análise ampla dos impactos. São Paulo: Thomson Reuters Brasil, 2020.

SETIC
Superintendência Estadual de
Tecnologia da Informação e Comunicação

Governo do Estado de
RONDÔNIA

(69) 3212-9546
VoIP: 9546

gab@setic.ro.gov.br
encarregadolgpd@setic.ro.gov.br

Av. Farquar, 2986 - Bairro Pedrinhas
CEP 76.801-470, Porto Velho – Rondônia
Palácio Rio Madeira, Anexo Rio Cautário, 6º Andar.